ON PAC EXTENSIONS AND SCALED TRACE FORMS

LIOR BARY-SOROKER AND DUBI KELMER

Abstract. Any non-degenerate quadratic form over a Hilbertian field (e.g., a number field) is isomorphic to a scaled trace form. In this work we extend this result to more general fields. In particular, prosolvable and prime-to-p extensions of a Hilbertian field. The proofs are based on the theory of PAC extensions.

1. Introduction and results

Let F/K be a finite separable field extension. It is equipped with a *trace form*, $x \mapsto \mathrm{Tr}_{F/K}(x^2)$. The characterization of trace forms has been initiated by Conner and Perlis, who were interested in the following question: Which quadratic forms over $\mathbb{Q}$ are Witt-equivalent to a trace form. In [3], they showed that these forms are precisely the positive non-degenerate quadratic forms (where positive means signature ≥ 0). This result was generalized to number fields [9], and to some Hilbertian fields [8]. In [4], Epkenhans showed that over a number field any non-degenerate positive quadratic form of dimension ≥ 4 is isomorphic to a trace form, and classified all classes of trace form of dimension ≤ 3, completing the work of Krüskemper [7].

There is a natural generalization of the trace form, that is, the *scaled trace form*. Namely, any separable extension F/K and any nonzero element $\alpha \in F$ admits the non-degenerate quadratic form

$$x \mapsto \mathrm{Tr}_{F/K}(\alpha x^2), \qquad x \in F.$$

A natural question is the following. Given a field K, can any non-degenerate quadratic form over K be realized as a scaled trace form.

In [9, 10], Scharlau and Waterhouse, independently, gave a positive answer for number fields or more generally for Hilbertian fields of characteristic $\neq 2$. Recall that a Hilbertian field K is a field with the property that for any irreducible polynomial $f(T,X)$ over $K(T)$ there exist infinitely many $a \in K$ for which $f(a,X)$ is irreducible.

Theorem (Scharlau-Waterhouse)**.** *Any non-degenerate quadratic form over a Hilbertian field of characteristic $\neq 2$ is isomorphic to a scaled trace form.*

In this note, we generalize this result to a larger class of fields. Note that an obvious necessary condition for a quadratic form of dimension n over K to be isomorphic to a scaled trace form is that K has a separable extension of degree n. Thus, a more subtle question is the following:

Question 1. Given a field K having a separable extension of degree n, can any non-degenerate quadratic form of dimension n over K be realized as a scaled trace form.

Remark 1.1. In general the answer to this question is negative. For example, $\mathbb{R}$ has a unique separable extension, $\mathbb{C}$, of degree 2. Any scaled trace form $x \mapsto \mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(\alpha x^2)$ is isotropic (since for $x = \sqrt{i/\alpha}$ we have $\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(\alpha x^2) = \mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(i) = 0$). Hence, the non-isotropic quadratic form $\langle 1, 1\rangle$ is not isomorphic to a scaled form.

Prosolvable extensions. An extension K/K_0 is called prosolvable, if any finite subextension L_0/K_0 (with $L_0 \subseteq K$) is solvable, i.e., the Galois group of the Galois closure of L_0/K_0 is solvable.

Theorem 1. *Let K be a prosolvable extension of a Hilbertian field of characteristic $\neq 2$. Then every non-degenerate quadratic form over K of dimension > 4 is isomorphic to a scaled trace form.*

Note that there are solvable extensions having no separable extensions of degree ≤ 4 (e.g., the maximal solvable extension), so in this generality the condition on the dimension is necessary. For prosolvable extension and quadratic forms of dimension $n = 3, 4$, we do not know the answer for Question 1. However in case $n = 2$ we show that the answer is negative (Proposition 3.5).

Prime-to-p extensions. Let p be a prime number. An algebraic extension K/K_0 is called prime-to-p, if p does not divide the degree of any finite subextension L_0/K_0 (with $L_0 \subseteq K$).

Theorem 2. *Let p be a prime and let K be a separable extension of a Hilbertian field K_0 of characteristic $\neq 2$ such that the Galois closure of K/K_0 is prime-to-p over K_0. Then every non-degenerate quadratic form over K is isomorphic to a scaled trace form.*

Notice that for $p = 2$ and quadratic forms of dimension > 4, Theorem 2 is a special case of Theorem 1. (Recall that, by the famous Feit-Thompson theorem, any group of odd order is solvable.)

PAC fields. Hilbert's Nullstellensatz asserts that every variety defined over an algebraically closed field K has a (K-rational) point. A field satisfying this property is called Pseudo Algebraically Closed (abbreviated PAC). An equivalent condition for a field K to be PAC is that any absolutely irreducible polynomial in two variables $f(X,Y)$ with coefficients in K has infinitely many roots $(x,y) \in K^2$ [5, Theorem 11.2.3]. There are abundance of PAC fields, in fact, in some sense most algebraic extensions of a countable Hilbertian field with a finitely generated absolute Galois group are PAC [5, Theorem. 18.6.1]. Over PAC fields we give a positive answer to Question 1.

Theorem 3. *Let K be a PAC field of characteristic $\neq 2$. A non-degenerate quadratic form of dimension n over K is isomorphic to a scaled trace form if and only if K has a separable extension of degree n.*

PAC extensions. In [6], Jarden and Razon generalized the notion of PAC fields to field extensions: A field extension M/K is said to be a **PAC extension** if for any absolutely irreducible polynomial in two variables $f(X,Y) \in M[X,Y]$, separable in Y (i.e., $\frac{\partial f}{\partial X} \neq 0$) there are infinitely many $(x,y) \in K \times M$ such that $f(x,y) = 0$. Clearly, a field K is PAC (as a field) if and only if the trivial extension K/K is PAC (as an extension). On the other hand, we note that a field extension M/K with M a PAC field is not necessarily a PAC extension, see [1, Page 9]. For fields having a PAC extension we give a partial answer for Question 1.

Theorem 4. *Let K be a field of characteristic $\neq 2$. Assume that K has a PAC extension M/K which has a separable extension of degree n. Then every non-degenerate quadratic form of dimension n over K is isomorphic to a scaled trace form.*

This theorem is the main theorem of the paper and we deduce all the previous theorems from it. For this deduction, we use the result of Jarden and Razon showing that, as for PAC fields, most algebraic extensions of a countable Hilbertian field with a finitely generated absolute Galois group are PAC extensions [6, Proposition 3.1].

Outline. In section 2 we prove Theorem 4. The proof goes along the lines of Scharlau-Waterhouse, where the use of Hilbertianity is replaced by a weaker property (Lemma 2.3). In order to apply this property, we have to compute the Galois group of the characteristic polynomial of a generic symmetric matrix times some diagonal matrix. Theorem 3 is then an obvious result of Theorem 4 (by taking $M = K$). In section 3 we use the abundance of PAC extensions over a Hilbertian field to deduce Theorems 1 and 2 from Theorem 4. In what follows all fields are assumed to have characteristic $\neq 2$.

Acknowledgments. We thank Ido Efrat, Dan Haran, Moshe Jarden, and Zeév Rudnick for helpful comments on an earlier draft of this paper. This work is part of the first author's Ph.D. thesis done at Tel Aviv University, supervised by Prof. Dan Haran.

2. Proof of Theorem 4

We start with a few auxiliary lemmata. The first lemma is a known result from the theory of Hermitian forms, giving a condition for a quadratic form to be isomorphic to a scaled trace form.

Lemma 2.1. *A nonzero symmetric matrix $D \in \mathrm{Mat}_n(K)$ represents a scaled trace form over K if and only if there is another symmetric matrix $A \in \mathrm{Mat}_n(K)$ such that the characteristic polynomial of AD is separable and irreducible over K.*

Proof. See e.g. [9, 10]. □

Let $D = \mathrm{diag}(d_1, \dots, d_n)$ be a diagonal matrix with $d_i \neq 0$ over some field. Let $T = (t_{ij})$ be a generic $n \times n$ symmetric matrix, i.e., the only algebraic relations are $t_{ij} = t_{ji}$. Let $p(\mathbf{t}, x)$ be the characteristic polynomial of TD, that is $p(\mathbf{t}, x) = \det(xI - TD)$.

Lemma 2.2. *Let L be a field such that $d_i \in L$, $i = 1, \dots, n$. Then $p(\mathbf{t}, x)$ is a separable irreducible polynomial over $L(\mathbf{t})$ and the Galois group of $p(\mathbf{t}, x)$ over $L(\mathbf{t})$ is the symmetric group S_n.*

Proof. The assertion is trivial for $n = 1$. For $n = 2$ the polynomial is separable and irreducible (and the Galois group is $S_2 \cong \mathbb{Z}/2\mathbb{Z}$) if and only if the discriminant Δ is not in the field $L(\mathbf{t})$. We can write explicitly $\Delta^2 = d_1^2 t_{11}^2 + d_2^2 t_{22}^2 + 4 d_1 d_2 t_{12}^2 - 2 d_1 d_2 t_{11} t_{22}$ which is not a square in $L(\mathbf{t})$. Let $n \geq 3$. Consider the ideals $\mathfrak{a}_1 = (t_{12}, \dots, t_{1n})$ and $\mathfrak{a}_2 = (t_{1n}, \dots, t_{(n-1)n})$ which correspond to the respective substitutions $t_{12} = \cdots = t_{1n} = 0$ and $t_{1n} = \ldots = t_{(n-1)n} = 0$. Let p_1, p_2 be the reduction of p modulo $\mathfrak{a}_1, \mathfrak{a}_2$ respectively. As $TD \equiv \left(\begin{array}{c|ccc} d_1 t_{11} & & & \\ \hline & d_2 t_{22} & \cdots & d_n t_{2n} \\ & \vdots & & \vdots \\ & d_2 t_{2n} & \cdots & d_n t_{nn} \end{array}\right) \bmod \mathfrak{a}_1$ the polynomial p_1 decomposes as $p_1(\mathbf{t}, x) = (x - d_1 t_{11}) h(\mathbf{t}, x)$ in $L[\mathbf{t}, x]/\mathfrak{a}_1 = L[t_{1,1}, t_{ij}, x \mid j \geq i \geq 2]$.

By induction, h, which is the characteristic polynomial of the lower block, is a separable irreducible polynomial with Galois group S_{n-1} over $L(t_{i,j} \mid j \geq i \geq 2)$. In particular $p(\mathbf{t}, x)$ is also separable.

Now assume that $p(\mathbf{t}, x)$ is reducible in $L[\mathbf{t}, x]$, namely

$$p(\mathbf{t}, x) = f(\mathbf{t}, x)g(\mathbf{t}, x),$$

where f and g are monic in x and $1 \leq \deg_x f \leq \deg_x g$. Then the irreducibility of h implies that $f \equiv x - d_1 t_{11} \pmod{\mathfrak{a}_1}$. A similar argument (for $p \mod \mathfrak{a}_2$) implies $f \equiv x - d_n t_{nn} \pmod{\mathfrak{a}_2}$. Consequently, we get that

$$f(\mathbf{t}, x) - (x - d_1 t_{11}) \in \mathfrak{a}_1 \quad \text{and} \quad f(\mathbf{t}, x) - (x - d_n t_{nn}) \in \mathfrak{a}_2,$$

hence $d_1 t_{11} - d_n t_{nn} \in \mathfrak{a}_1 + \mathfrak{a}_2$, a contradiction.

Finally, we calculate the Galois group G of $p(\mathbf{t}, x)$ over $L(\mathbf{t})$: As $p_1 = (x - d_1 t_{11})h(\mathbf{t}, x)$ in $L[\mathbf{t}, x]/\mathfrak{a}_1$ and the polynomials are separable, there exists a bijection between the roots of p and the roots of p_1. Such a bijection induces an embedding of the Galois group of h over $L(t_{ij} \mid j \geq i \geq 2)$ into G via the action on the respective roots (c.f., [5, Lemma 6.1.4]). That is $S_{n-1} \leq G \leq S_n$ under a suitable labeling of the roots. As $p(\mathbf{t}, x)$ is separable and irreducible, G is transitive, and hence $G = S_n$. Indeed, for any $\sigma \in S_n$ there exists $\tau \in G$ such that $\sigma(n) = \tau(n)$, so $\sigma \in \tau S_{n-1} \subseteq G$. □

The next lemma is a weak Hilbert's Irreducibility Theorem for PAC extensions.

Lemma 2.3. *Let M/K be a PAC extension, let $f(t_1, \ldots, t_s, x) \in M[t_1, \ldots, t_s, x]$ be a separable polynomial of degree n in x, and let $\tilde{M}$ be an algebraic closure of M. Assume that the Galois group of $f(t_1, \ldots, t_s, x)$ over $\tilde{M}(t_1, \ldots, t_s)$ is the symmetric group S_n. Then there exist infinitely many $(\alpha_1, \ldots, \alpha_s) \in K^s$ such that $f(\alpha_1, \ldots, \alpha_s, x)$ is irreducible over M, provided that M has a separable extension of degree n.*

The proof appears in [1, Cor. 2] (the proof is given for $s = 1$, but it is easy to check that the same proof works for $s > 1$).

Proof of Theorem 4. Let M/K be a PAC extension of characteristic $\neq 2$ and let Q be a non-degenerate quadratic form over K. Choose a basis in which Q is diagonal and denote by D the corresponding diagonal matrix. By Lemma 2.1, it suffices to find a symmetric matrix A (with coefficients in K) such that AD has an irreducible characteristic polynomial. For that, take T to be the generic symmetric matrix with indeterminate coefficients. By Lemma 2.2 (with $L = \tilde{M}$) the characteristic polynomial, $p(\mathbf{t},x)$, of TD satisfies the condition of Lemma 2.3. Thus if M has a separable extension of degree n, we can specialize $\mathbf{t}\mapsto\mathbf{a}\in K^{n^2}$ such that $p(\mathbf{a},x)$ is irreducible. We thus get, for the specialized matrix $A=(a_{ij})$, that AD has an irreducible characteristic polynomial. □

3. Fields with PAC extensions

In order to deduce Theorems 1 and 2 from Theorem 4, we need to show that the fields in question have a PAC extension having suitable separable extensions. We start by citing some results regarding PAC extensions that we will need.

Let K_0 be a field and $e\geq 1$ an integer. For $\boldsymbol{\sigma}=(\sigma_1,\dots,\sigma_e)\in\mathrm{Gal}(K_0)^e$, we denote by $\langle\boldsymbol{\sigma}\rangle=\langle\sigma_1,\dots,\sigma_e\rangle$ the closed subgroup of $\mathrm{Gal}(K_0)$ generated by the coordinates of $\boldsymbol{\sigma}$, and by $K_{0s}(\boldsymbol{\sigma})$ the fixed field of $\langle\boldsymbol{\sigma}\rangle$ in a fixed separable closure K_{0s} of K_0. We recall that the absolute Galois group of K_0 is profinite (in particular compact), and hence equipped with a probability Haar measure.

Proposition 3.1. *Let K_0 be a countable Hilbertian field and K/K_0 an algebraic extension.*

a. *For almost all $\boldsymbol{\sigma}\in\mathrm{Gal}(K_0)^e$ the extension $K_{0s}(\boldsymbol{\sigma})/K_0$ is a PAC extension and $\langle\boldsymbol{\sigma}\rangle$ is a free profinite group of rank e (*[6, Proposition 3.1] *and* [5, Theorem 18.5.6]*).*
b. *If M_0/K_0 is a PAC extension, then so is M_0K/K (*[6, Corollary 2.5]*).*

We shall also use the following simple group theoretic lemma.

Lemma 3.2. *Let $N\leq N_0\leq G$ be profinite groups such that N is normal in G. Let H be a quotient of G such that H and G/N have no common nontrivial quotients. Then, H is a quotient of N_0. In particular, if H has an open subgroup of index n, so does N_0.*

Proof. Let $U\lhd G$ such that $G/U=H$. Since G/NU is a common quotient of G/U and G/N, we get that $G/NU=1$, so $G=NU$. Therefore also $N_0U=G$, and hence $N_0/N_0\cap U\cong N_0U/U=G/U=H$. □

3.1. Prosolvable extensions.

The following proposition shows that prosolvable extensions of a countable Hilbertian field have many PAC extensions (cf. [1, Corollary 3.7]).

Proposition 3.3. *Let K be a prosolvable extension of a countable Hilbertian field K_0 and $e\geq 2$. Then for almost all $\boldsymbol{\sigma}\in\mathrm{Gal}(K_0)^e$ the field $M=KK_{0s}(\boldsymbol{\sigma})$ is a PAC extension of K and it has a separable extension of every degree >4.*

Proof. Let $\hat{K}$ be the Galois closure of K/K_0, so $\mathrm{Gal}(\hat{K}/K_0)$ is prosolvable. For almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K_0)^e$ the field $M_0 = K_{0s}(\sigma)$ is a PAC extension of K_0 and its absolute Galois group $G = \langle \boldsymbol{\sigma} \rangle$ is a free profinite group of rank e (Proposition 3.1a.). Fix such a $\boldsymbol{\sigma}$ and write $M = KK_{0s}(\boldsymbol{\sigma})$. Then M/K is PAC (Proposition 3.1b.). Let $N_0 = \mathrm{Gal}(M)$ be the absolute Galois group of M and let $N = \mathrm{Gal}(\hat{K}K_{0s}(\boldsymbol{\sigma}))$. Then $N \le N_0 \le G$, N is normal in G, and $G/N = \mathrm{Gal}(\hat{K}K_{0s}(\boldsymbol{\sigma})/K_0)$. The restriction map $G/N \to \mathrm{Gal}(\hat{K}/K_0)$ is an embedding, so G/N is prosolvable.

Let $n > 4$, we show that M has a separable extension of degree n. By Galois correspondence, it suffices to show that N_0 has an open subgroup of index n. As G is free of rank ≥ 2 it has A_n (the alternating group) as a quotient. A_n and G/N have no nontrivial common quotients (as G/N is prosolvable and A_n is simple). Now Lemma 3.2 with $H = A_n$ implies that N_0 has an open subgroup of index n (since $(A_n : A_{n-1}) = n$). □

Proof of Theorem 1. Let K be a prosolvable extension of a Hilbertian field K_0. In case K is countable, the assertion follows immediately from Theorem 4 and the above proposition. When K is uncountable, the assertion follows from the countable case by the Löwenheim-Skolem Theorem [5, Proposition 7.4.2].

Indeed, let $\mathcal{L}$ be the language of Rings together with a unary predicate P. By Löwenheim-Skolem, there exists a countable elementary substructure E/E_0 of the structure K/K_0, in particular, E/E_0 is a field extension. We show that E_0 is Hilbertian and that E/E_0 is prosolvable. This would imply that every non-degenerate quadratic form over E is isomorphic to a scaled trace form. Since, for any fixed positive integer n, the statement "All quadratic forms of dimension n are isomorphic to scaled trace forms" is elementary (by Lemma 2.1), this would conclude the proof.

To show that E_0 is Hilbertian, we need to show that for every positive integer n, every irreducible polynomial $f(T, X)$ of degree n has an irreducible specialization. For any fixed n this is an elementary statement which is true in K_0 and hence also in E_0. Next, we show that E/E_0 is separable algebraic and that the Galois closure $\hat{E}$ of E/E_0 is linearly disjoint from K_0 over E_0. Indeed, if $x \in E$, then $x \in K$. Hence there exists an irreducible separable polynomial f over K_0 satisfying $f(x) = 0$. The latter statement is elementary, so x is separable and algebraic over E_0. Now let L be a finite separable extension of E_0 and f an irreducible generating polynomial of L/E_0. Then f generates LK_0/K_0 and is also irreducible over K_0 (since it is elementary). Therefore $[L : E_0] = \deg f = [LK_0 : K_0]$, i.e., L is linearly disjoint from K_0 over E_0.

As L is an arbitrary finite separable extension, we get that E_{0s} is linearly disjoint from K_0 over E_0, and in particular so is $\hat{E}$. Finally, let $\hat{K}$ be the Galois closure of K/K_0. Then $\hat{E}K_0 \subseteq \hat{K}$, and $\mathrm{Gal}(\hat{E}/E_0) \cong \mathrm{Gal}(\hat{E}K_0/K_0)$ via restriction. As $\mathrm{Gal}(\hat{K}/K_0)$ is prosolvable, so is $\mathrm{Gal}(\hat{E}K_0/K_0) \cong \mathrm{Gal}(\hat{K}/K_0)/\mathrm{Gal}(\hat{K}/\hat{E}K_0)$, and hence $\mathrm{Gal}(\hat{E}/E_0)$ is prosolvable. □

Remark 3.4. Theorem 1 is valid in particular for the maximal prosolvable extension $\mathbb{Q}_{\mathrm{sol}}$ of $\mathbb{Q}$. However, $\mathbb{Q}_{\mathrm{sol}}$ has no quadratic extensions, hence there is a unique non-degenerate quadratic form of a given dimension (up to isomorphism). So in this maximal case the theorem is obvious.

Theorem 1 answers Question 1 positively for solvable extensions and quadratic forms of dimension $n > 4$. The following proposition shows that for $n = 2$ the answer is negative. We do not know what happens in the gap $n = 3, 4$.

Proposition 3.5. *There exists a prosolvable extension $K/\mathbb{Q}$ which has an extension of degree 2, but the non-degenerate quadratic form $\langle 1, 1\rangle$ is not isomorphic to a scaled trace form over K.*

Proof. Fix an embedding of $\mathbb{Q}$ in $\mathbb{C}$. Complex conjugation acts nontrivially on $\mathbb{Q}_{\mathrm{sol}}$. Let K be its fixed field, i.e., $K = \mathbb{Q}_{\mathrm{sol}} \cap \mathbb{R}$. Then $[\mathbb{Q}_{\mathrm{sol}} : K] = 2$. Also if L/K is an extension of degree 2, then L is also a prosolvable extension of $\mathbb{Q}$, so $L \subseteq \mathbb{Q}_{\mathrm{sol}}$, which implies that $L = \mathbb{Q}_{\mathrm{sol}}$. Thus $\mathbb{Q}_{\mathrm{sol}}$ is the unique extension of degree 2 over K. We now proceed as in $\mathbb{C}/\mathbb{R}$. Any scaled trace form $x \mapsto \mathrm{Tr}_{\mathbb{Q}_{\mathrm{sol}}/K}(\alpha x^2)$ is isotropic (since $x = \sqrt{i/\alpha} \in \mathbb{Q}_{\mathrm{sol}}$). The assertion follows since $\langle 1, 1\rangle$ is not isotropic over K (recall that K is real). □

3.2. **Prime-to-p extensions.** Let p, m, k be positive integers such that p is prime, $p \nmid m$, and $p \mid \varphi(m)$. Here φ is Euler's totient function. Consider the semidirect product $H = \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/p^k\mathbb{Z}$ of all pairs (a, x), $a \in \mathbb{Z}/m\mathbb{Z}$ and $x \in \mathbb{Z}/p^k\mathbb{Z}$ with multiplication given by

$$(a, x)(b, y) = (a + \alpha^x b, x + y),$$

where $\alpha \in (\mathbb{Z}/m\mathbb{Z})^*$ is a fixed element of (multiplicative) order p. In particular

$$(a, x)^n = (a(1 + \alpha + \alpha^2 + \cdots + \alpha^n), nx) = \left(\frac{a(1 - \alpha^{n+1})}{1 - \alpha}, nx\right).$$

We embed $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}/p^k\mathbb{Z}$ in H in the natural way.

Lemma 3.6. *Let p, m, k, and $H = \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/p^k\mathbb{Z}$ be as above. Then*

a. *H is generated by its p-sylow subgroups.*

b. *The only prime-to-p quotient of H is trivial.*
c. *If $n \mid m$, then there exist subgroups H_0 and H_1 of H of respective indices $p^k n$ and n.*

Proof. The elements $(0,1)$ and $(1,1)$ generate H, so for a., it suffices to show that their order divides p^k (and hence is p^k). We have $(0,1)^{p^k} = (0,p^k) = (0,0)$. Now, since $\alpha^{p^k} = (\alpha^p)^k = 1$, we have

$$(1,1)^{p^k} = \left(\frac{1-\alpha^{p^k}}{1-\alpha}, 0\right) = (0,0).$$

b. follows from a.: Indeed, let $\bar{H} = H/N$ be a quotient of H with order prime-to-p. Thus p^k divides the order of N, and hence N contains a p-sylow subgroup of H. As $N \lhd H$, it contains all the p-sylow subgroups. By a., $N = H$ and $\bar{H} = 1$, as desired.

To show c., assume $n \mid m$. Let H_0 be the kernel of the natural map $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Then $H_0 \le \mathbb{Z}/m\mathbb{Z} \le H$. Note that H_0 is invariant under the action of $\mathbb{Z}/p^k\mathbb{Z}$ (i.e., $a \in H_0 \Rightarrow \alpha a \in H_0$) and define $H_1 = H_0 \rtimes \mathbb{Z}/p^k\mathbb{Z}$. Now,

$$(H : H_0) = (H : \mathbb{Z}/m\mathbb{Z})(\mathbb{Z}/m\mathbb{Z} : H_0) = p^k n$$

and $(H : H_1) = n$, as desired. □

Proposition 3.7. *Let p be a prime, let K be a separable extension of a countable Hilbertian field K_0 such that the Galois closure is prime-to-p over K_0. Let $e \ge 2$. Then for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K_0)^e$ the field $M = KK_{0s}(\boldsymbol{\sigma})$ is a PAC extension of K and it has a separable extension of every degree.*

Proof. Let $\hat{K}$ be the Galois closure of K/K_0, so every finite quotient of $\mathrm{Gal}(\hat{K}/K_0)$ has order prime to p. As in the proof of Proposition 3.3, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K_0)^e$ the field $M_0 = K_{0s}(\boldsymbol{\sigma})$ has a free absolute Galois group of rank e, namely $G = \langle \boldsymbol{\sigma} \rangle$, and $M = M_0 K$ is a PAC extension of K. Let $N_0 = \mathrm{Gal}(M)$ be the absolute Galois group of M and let $N = \mathrm{Gal}(\hat{K}K_{0s}(\boldsymbol{\sigma}))$. Then $N \le N_0 \le G$, N is normal in G, and $G/N = \mathrm{Gal}(\hat{K}K_{0s}(\boldsymbol{\sigma})/K_0)$. The restriction map $G/N \to \mathrm{Gal}(\hat{K}/K_0)$ is an embedding, so every finite quotient of G/N has order prime to p (because it is a subgroup of a finite quotient of $\mathrm{Gal}(\hat{K}/K_0)$).

By Galois correspondence, it suffices to show that N_0 has open subgroups of any index. Let n be a positive integer prime to p and $k \ge 1$. Let l be a prime number such that $l \nmid n$ and $p \mid l-1$ and let $m = nl$ (such a prime l exists since there are infinitely many primes in the arithmetic progression $l \equiv 1 \pmod{p}$). Then $p \nmid m$ and $p \mid \varphi(m)$. Let $H = \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/p^k\mathbb{Z}$ as in Lemma 3.6. Then H and G/N have no nontrivial common quotients (by Lemma 3.6b.). By Lemma 3.2 and Lemma 3.6c., N_0 has open subgroups of index n and np^k, i.e., of any index. □

Proof of Theorem 2. For a countable field K, Theorem 2 follows immediately from Theorem 4 and the above proposition. For an uncountable field the theorem follows from the Löwenheim-Skolem Theorem (as in the proof of Theorem 1). □

3.3. **A remark.** In this work we saw that the property for a field K to have PAC extension with separable extension of degree n, implies that every non-degenerate quadratic form of dimension n is isomorphic to a scaled trace form. This leads to the problem of classifying fields K which have a PAC extension with a separable extension of a given degree. This is a refinement of [1, Problem 3.9], raised in relation to Dirichlet's theorem for polynomial rings in one variable.

References

1. L. Bary-Soroker, *Dirichlet's theorem for polynomial rings*, manuscript.
2. L. Bary-Soroker and M. Jarden, *PAC fields over finitely generated fields*, manuscript.
3. P.E. Conner and R. Perlis, *A survey of trace forms of algebraic number fields*, Singapore: World Scientific Publ. 1984.
4. M. Epkenhans, *On trace forms of algebraic number fields*, Arch. Math. (Basel) 60 (1993), no. 6, 527–529.
5. M. D. Fried and M. Jarden, *Field arithmetic*, second ed., revised and enlarged by Moshe Jarden, Ergebnisse der Mathematik (3) **11**, Springer-Verlag, Heidelberg, 2005.
6. M. Jarden and A. Razon, *Pseudo algebraically closed fields over rings*, Israel J. Math. **86** (1994), no. 1-3, 25–59.
7. M. Krüskemper, *Algebraic number field extensions with prescribed trace form*, J. Number Theory 40 (1992), no. 1, 120124.
8. M. Krüskemper and W. Scharlau, *On trace forms of Hilbertian fields*, Comment. Math. Helv. **63** (1988), no. 2, 296–304.
9. W. Scharlau, *On trace forms of algebraic number fields*, Math. Z. **196** (1987), no. 1, 125–127.
10. W. C. Waterhouse, *Scaled trace forms over number fields*, Arch. Math. (Basel) **47** (1986), no. 3, 229–231.

The Raymond and Beverly Sackler School of Mathematical Sciences Tel Aviv University Ramat Aviv, Tel Aviv 69978 ISRAEL
E-mail address: `barylior@post.tau.ac.il`

The Raymond and Beverly Sackler School of Mathematical Sciences Tel Aviv University Ramat Aviv, Tel Aviv 69978 ISRAEL
E-mail address: `kelmerdu@post.tau.ac.il`